(54) Protected box for checking a personal identification number

(57) The box (6) of a unit for typing of a personal identification number houses internally a printed circuit of which the top carries a keypad (2) and a display (3) while the bottom accommodates a protected module, linked in particular to the keypad and capable of checking the number or transmitting it in encrypted form, using secret data kept in a backed-up random access memory (18). The micro-switches (5) are placed inside the box (6) to remain closed when the two parts of this box are joined together. The inside of the box is passed through by a live wire (4). The power supply circuit of the backed-up random access memory (18) passes through the micro-switches (5) and this live wire (4).

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 596 176**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **86 03945**

(51) Int Cl⁴ : G 06 K 5/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19 mars 1986.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 39 du 25 septembre 1987.

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *ELECTRONIQUE SERGE DASSAULT, Société Anonyme.* — FR.

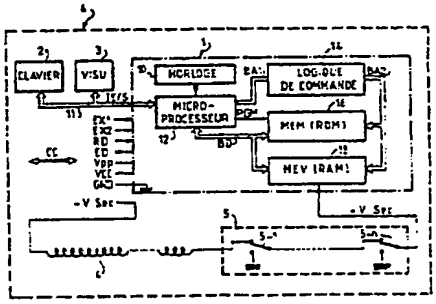
(72) **Inventeur(s) :** Joël Soupirot.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** Cabinet Netter.

(54) Boîtier protégé pour le contrôle d'un code confidentiel.

(57) Le boîtier 6 d'une unité pour la composition d'un code confidentiel loge intérieurement un circuit imprimé dont le dessus porte un clavier 2 et une visualisation 3, tandis que le dessous reçoit un module protégé, relié notamment au clavier, et propre à vérifier le code ou à le transmettre sous forme chiffrée, à l'aide de données secrètes conservées en mémoire vive sauvegardée 18. Les micro-interrupteurs 5 sont placés à l'intérieur du boîtier 6 pour demeurer fermés lorsque les deux parties de ce boîtier sont réunies. L'intérieur du boîtier est parcouru par un fil conducteur 4. Le circuit d'alimentation de la mémoire vive sauvegardée 18 passe par les micro-interrupteurs 5 et ce fil conducteur 4.



FR 2 596 176 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

Boîtier protégé pour le contrôle d'un code confidentiel.

L'invention concerne les appareils de paiement électronique, que l'on appelle aussi terminaux de point de vente, ou terminaux d'encaissement.

Ces appareils sont installés chez les commerçants, pour permettre d'automatiser les transactions par carte de paiement. Pour ce qui le concerne, le client peut ratifier la transaction par sa signature, ou bien par la composition de son code confidentiel, sur un petit appareil séparé, dit boîtier client.

Des précautions poussées sont prises pour conserver la confidentialité de ce code :

- ou bien, il est vérifié sur place, par des moyens de contrôle appropriés incorporés au boîtier du client; aucune transmission du code confidentiel en dehors du boîtier client n'est alors requise;

- ou bien, ce code est vérifié dans un ordinateur central, auquel cas, il ne sort du boîtier client qu'après avoir subi un chiffrement, qui le rend pratiquement indécryptable.

Ces deux fonctions sont maintenant assurées par un circuit intégré hybride, protégé de résine, qui fait partie du

boîtier client. Bien entendu, les moyens de contrôle ou de chiffrement utilisés par ce circuit sont tenus secrets.

Ainsi, un degré de sécurité élevé est atteint.

Cependant, la Demanderesse a observé que des personnes malveillantes pourraient tenter d'intercepter un code confidentiel, au moment où il passe du clavier au circuit intégré protégé.

La présente invention a pour but d'améliorer la sécurité sur ce point. Pour cela, l'invention a été développée pour une unité permettant le contrôle d'un code confidentiel, et comprenant un boîtier, en deux parties solidaires, qui loge intérieurement un circuit imprimé. La face supérieure de ce circuit imprimé porte un clavier, accessible sous abri à l'usager par la partie supérieure du boîtier. La face inférieure du circuit imprimé porte un module protégé, relié au clavier, et en principe à une visualisation, ainsi qu'à un câble de transmission vers un terminal de transaction automatique. Le module protégé, souvent constitué d'un circuit intégré hybride noyé dans la résine, est capable d'effectuer la vérification interne et/ou la transmission chiffrée d'un code confidentiel composé sur le clavier. Cette vérification se fait à l'aide de données secrètes conservées dans une mémoire vive sauvegardée, qui fait partie du module protégé.

Selon un premier aspect de l'invention, un ou des micro-interrupteurs sont placés à l'intérieur du boîtier, pour être fermés lorsque ses deux parties sont réunies (en théorie, un seul micro-interrupteur pourrait suffire mais la Demanderesse préfère actuellement prévoir plusieurs micro-interrupteurs); la partie inférieure du boîtier porte un fil conducteur qui la parcourt, au moins au voisinage des micro-interrupteurs; enfin, le circuit d'alimentation sauvegardé de la mémoire vive passe par les micro-interrupteurs et par ce fil conducteur.

De préférence, le fil conducteur parcourt quasi-complètement la surface interne de la partie inférieure du boîtier. Pour plus de sûreté, on prévoiera même qu'il parcourt aussi la partie supérieure du boîtier, au moins partiellement, en particulier sur les côtés.

Selon un autre aspect de l'invention, la partie inférieure du boîtier est renforcée intérieurement par une résine, et le fil conducteur est noyé dans cette résine, ou bien logé entre cette résine et la partie inférieure du boîtier. La gaîne d'isolation de ce fil est avantageusement de même couleur que la résine.

Selon un autre aspect, particulièrement intéressant de l'invention, la position des micro-interrupteurs est variable d'un boîtier à l'autre. Ceci peut être obtenu aisément en fixant des tolérances assez larges pour positionner ces micro-interrupteurs lors de la fabrication des boîtiers.

Ainsi, la position des micro-interrupteurs peut être rendue variable de quelques millimètres. Le fil conducteur peut alors parcourir la surface interne du boîtier avec un pas du même ordre, au moins dans une direction, de préférence de façon bidirectionnelle. L'implantation de ce fil peut se faire à la main sans coût excessif.

Selon encore un autre aspect de l'invention, dans son état ouvert, chaque micro-interrupteur met à la masse l'alimentation sauvegardée de la mémoire vive. On assure ainsi une disparition rapide du contenu de celle-ci.

Les micro-interrupteurs peuvent être disposés pour certains près des lèvres de collage des deux parties du boîtier, pour d'autres sur la face inférieure du circuit imprimé, ou encore entre des composants portés par cette face inférieure du circuit imprimé et le fond interne inférieur du boîtier.

Enfin, selon encore un autre aspect de l'invention, les liaisons électriques entre le clavier et le module protégé, qui sont relatives à l'état des touches, sont essentiellement réalisées par des pistes situées sur la face inférieure du circuit imprimé.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels :

- la figure 1 est une vue en perspective montrant un terminal de transaction relié par un câble à une unité de composition de code confidentiel, ou "boîtier client";

- la figure 2 est le schéma électrique de principe des circuits contenus à l'intérieur du boîtier client; et

- les figures 3A et 3B sont deux vues en coupe du boîtier client, selon un mode de réalisation de l'invention.

Les dessins annexés comportent des informations de caractère certain, ou bien géométriques. A ce titre, ils sont incorporés à la description non seulement pour éclairer celle-ci mais aussi pour contribuer le cas échéant à la définition de l'invention.

Sur la figure 1, la référence TCO désigne un terminal de transaction, qui peut être un terminal de paiement électronique (série E200 vendue par la Demanderesse), ou bien un terminal d'encaissement multi-commerces (série E300 vendue également par la Demanderesse).

Ce terminal est relié par un câble de connexion CC à un boîtier client BCL, dont le boîtier proprement dit 6 est surmonté d'un abri 30, propre à dissimuler aux regards indiscrets un clavier 2 et une visualisation 3.

Sur le schéma électrique de la figure 2, on retrouve en 6 les limites extérieures du boîtier. Le module protégé 1, qui est un circuit intégré hybride, comporte une horloge 10, reliée à un microprocesseur 12. Le bus d'adresses BA1 de celui-ci traverse une logique de commande 14, pour venir en BA2 vers une mémoire morte 16 (MEM ou ROM), ainsi qu'une mémoire vive 18 (MEV ou RAM).

Le câble de connexion CC est la seule liaison électrique qui traverse la paroi 6 du boîtier. Il comprend par exemple :

- une liaison d'alimentation Vcc

- une liaison de masse GND;

- une tension d'alimentation sauvegardée ou secourue notée VSec.

Selon l'invention, des micro-interrupteurs 5-1 à 5-n sont placés à l'intérieur du boîtier, pour être fermés (état illustré sur la figure 2) lorsque les deux parties du boîtier sont réunies. La partie inférieure du boîtier porte un fil conducteur 4 continu, qui la parcourt au moins au voisinage de ces micro-interrupteurs.

La figure 2 montre que le circuit d'alimentation sauvegardée de la mémoire vive, à partir de l'arrivée VSec, passe par le fil continu 4 et l'ensemble 5 des micro-interrupteurs. La tension Vseca disponible à la sortie de ce circuit série n'existera donc que si aucun des micro-interrupteurs n'est ouvert, et si le fil continu 4 n'a pas été coupé.

Le mode de réalisation illustré sur la figure 2 est actuellement préféré, mais on pourrait, inversement, placer d'abord les micro-interrupteurs 5 et ensuite le fil 4, près de la mémoire vive 18.

De préférence, pour assurer l'interruption totale de l'alimentation de la mémoire vive et l'effacement immédiat des données secrètes qu'elle contient, chacun des micro-interrupteurs 5-1 à 5-n va, lorsqu'il s'ouvre, mettre à la masse l'alimentation de cette mémoire vive, et ce après une faible excursion.

Les figures 3A et 3B illustrent en plus de détails, un mode de réalisation particulier de l'invention.

On reconnaît en 19 un circuit imprimé, dont la face supérieure porte des touches 2-1 à 2-7 du clavier 2. On sait maintenant réaliser un montage direct des touches d'un clavier sur un circuit imprimé. Sur la face inférieure du circuit imprimé 19 est monté, notamment, le circuit intégré hybride 1, dont le schéma détaillé est donné sur la figure 2.

Les liaisons électriques entre le clavier 2 et le module protégé 1, qui ne passent pas par une interface standard, comportent, sous forme matricielle :

- des liaisons de scrutation des touches ("lignes")

- des liaisons relatives à l'état des touches ("colonnes").

Selon l'invention, les liaisons électriques relatives à l'état des touches sont essentiellement réalisées par des pistes situées sur la face inférieure du circuit imprimé 19, à l'exclusion de toute piste sur la face supérieure de ce circuit imprimé. Aucun accès à ces liaisons n'est donc possible par la face supérieure du circuit imprimé.

On pourra trouver avantage à faire de même pour les liaisons de scrutation des touches.

Le boîtier 6 est constitué d'une partie inférieure 60, et d'une partie supérieure 61, dont le dessus est plat en 62 et entouré par la bride 30;

La partie inférieure du boîtier 60 est renforcée par une résine dure 65. Un fil conducteur continu 40 est noyé dans une résine, ou logé entre cette résine 65 et la partie inférieure 60 du boîtier.

Pour une protection encore meilleure, on prévoit également un revêtement intérieur de résine 66 au moins sur les côtés de la partie supérieure 61 du boîtier. Un fil continu 41, relié en série avec le fil 40, est prévu dans cette résine 66, ou entre celle-ci et la paroi 61, comme précédemment.

Près de la lèvre 68, formant jonction collée entre les deux parties 60 et 61 du boîtier, sont montés intérieurement deux micro-interrupteurs 5-1 et 5-2, à l'avant du boîtier, et à l'arrière deux autres micro-interrupteurs, dont seul l'un, 5-3, est visible sur la figure 3A.

Dans le mode de réalisation illustré, ces micro-interrupteurs sont montés dans des logements définis dans les blocs de résine 65 et 66.

La figure 3B montre également que des micro-interrupteurs tels 5-5 peuvent être montés entre la face inférieure du circuit imprimé 19 et le fond interne inférieur du boîtier, défini ici par le bloc de résine 65.

Comme montré en 5-6, on pourrait encore prévoir des micro-interrupteurs montés entre des composants portés par la face inférieure du circuit imprimé (notamment le module protégé 1) et le fond interne inférieur du boîtier.

Enfin un ou des microinterrupteurs placés sous la paroi 62, avec interposition d'un masque au format du clavier, permettent de détecter toute tentative de découpe au niveau des touches.

Il est concevable, mais onéreux, de prévoir un assez grand nombre de micro-interrupteurs de ce genre placés en différentes parties du boîtier. Par principe, l'invention prévoit que les fils 40 ou 41 interdisent tout perçage ou autre brisure locale du boîtier, qui permettrait l'accès à un micro-interrupteur, et par conséquent la neutralisation de celui-ci (calage, collage, par exemple).

La Demanderesse a observé qu'il est plus simple de prévoir que la position des micro-interrupteurs soit variable d'un boîtier à l'autre, ce qui empêche toute prévision de la position exacte d'un tel micro-interrupteur. Cette mesure pourrait d'ailleurs en soi être suffisante pour assurer la protection du boîtier : en effet, si ce boîtier était largement percé en un endroit anormal, le client s'en rendrait compte, et pourrait refuser de s'en servir.

Cependant, la sécurité est considérablement renforcée par le fil continu 4, qui parcourt l'intérieur du boîtier avec un pas assez étroit, et de préférence dans les deux sens, ce pas étant rendu comparable aux variations de positions des micro-interrupteurs. Par exemple, la position des micro-interrupteurs varie de $\pm$ 2 mm, et le pas du fil est de 5 mm. Il devient alors pratiquement impossible de percer le boîtier pour tenter d'accéder à un micro-interrupteur, sans avoir entre temps ouvert le circuit d'alimentation de la mémoire sauvegardée.

Le résultat est alors que le boîtier client est strictement inutilisable. Comme il est par ailleurs prévu que le boîtier et le terminal sont la propriété des banques

émettrices, et qu'ils ne sont jamais réparés in situ, mais toujours échangés pour contrôle en atelier en cas d'anomalie, il devient ainsi pratiquement impossible d'intercepter le code confidentiel d'un usager, après avoir violé le boîtier prévu pour la composition de ce code, et modifié par exemple le câble de connexion.

Compte-tenu du sujet, il n'est pas souhaitable de développer complètement ici les avantages obtenus par la mise en oeuvre de l'invention. Le spécialiste comprendra comment la sécurité se trouve renforcée.

Bien entendu, la présente invention n'est pas limitée au mode de réalisation décrit. Elle s'étend au contraire à toute variante incluse dans le cadre des revendications ci-après.

En particulier, dans le cas où les états des touches n'apparaissent que sous le circuit imprimé, on peut alléger la protection.

Revendications

1. Unité permettant le contrôle d'un code confidentiel,

comprenant un boîtier (6), en deux parties solidaires (60, 61) qui loge intérieurement un circuit imprimé (19), dont la face supérieure porte un clavier (2), accessible sous abri à l'usager (62) par la partie supérieure (61) du boîtier, et dont la face inférieure porte un module protégé (1), relié au clavier (2) ainsi qu'à un câble de transmission (CC), et capable d'effectuer la vérification interne et/ou la transmission chiffrée d'un code confidentiel composé sur le clavier (2), à l'aide de données secrètes conservées dans une mémoire vive sauvegardée (18), laquelle fait partie du module protégé (1),

caractérisée en ce que des micro-interrupteurs (5) sont placés à l'intérieur du boîtier (6), pour être fermés lorsque ses deux parties (60, 61) sont réunies, en ce que la partie inférieure (60) du boîtier porte un fil conducteur (4) qui la parcourt au moins au voisinage des micro-interrupteurs (5), et en ce que le circuit (4, 5) d'alimentation sauvegardée de ladite mémoire vive passe par les micro-interrupteurs (5) et par ce fil conducteur (4).

2. Unité selon la revendication 1, caractérisée en ce que le fil conducteur (40) parcourt quasi complètement la surface interne de la partie inférieure du boîtier.

3. Unité selon la revendication 2, caractérisée en ce que la partie inférieure du boîtier (60) est renforcée par une résine (65), et en ce que le fil conducteur (40) est noyé dans cette résine ou logé entre cette résine et la partie inférieure du boîtier.

4. Unité selon l'une des revendications 1 à 3, caractérisé en ce que la position des micro-interrupteurs (5) est variable d'un boîtier à l'autre.

5. Unité selon la revendication 4, caractérisée en ce que la position des micro-interrupteurs (5) est variable de quelques millimètres, et en ce que le fil conducteur (4) parcourt la surface interne du boîtier avec un pas du même ordre.

6. Unité selon l'une des revendications 1 à 5, caractérisée en ce que, dans son état ouvert, chaque micro-interrupteur (5) met à la masse l'alimentation sauvegardée de la mémoire vive.

7. Unité selon l'une des revendications précédentes, caractérisée en ce que certains au moins des micro-interrupteurs (5) sont placés près des lèvres (68) de jonction des deux parties du boîtier.

8. Unité selon l'une des revendications précédentes, caractérisée en ce que certains au moins des micro-interrupteurs (5) sont montés sur la face inférieure du circuit imprimé (19).

9. Unité selon l'une des revendications précédentes, caractérisée en ce que certains au moins des micro-interrupteurs (5) sont montés entre des composants portés par la face inférieure du circuit imprimé, et le fond interne inférieur du boîtier (60, 65).

10. Unité selon l'une des revendications précédentes, caractérisée en ce que les liaisons électriques entre le clavier (2) et le module protégé (1) relatives à l'état des touches, sont essentiellement réalisées par des pistes situées sur la face inférieure du circuit imprimé.

FIG. 1

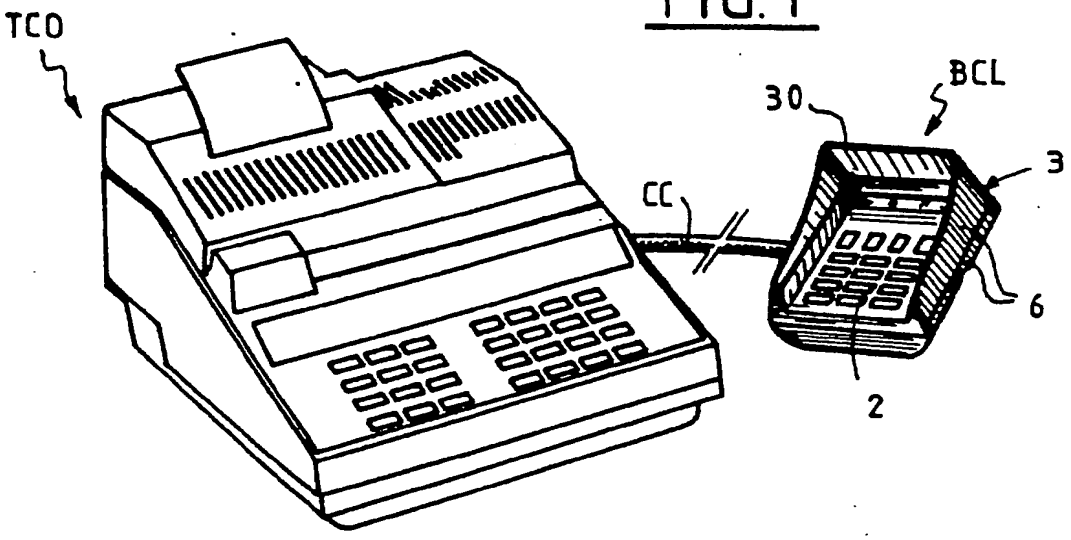


FIG. 2

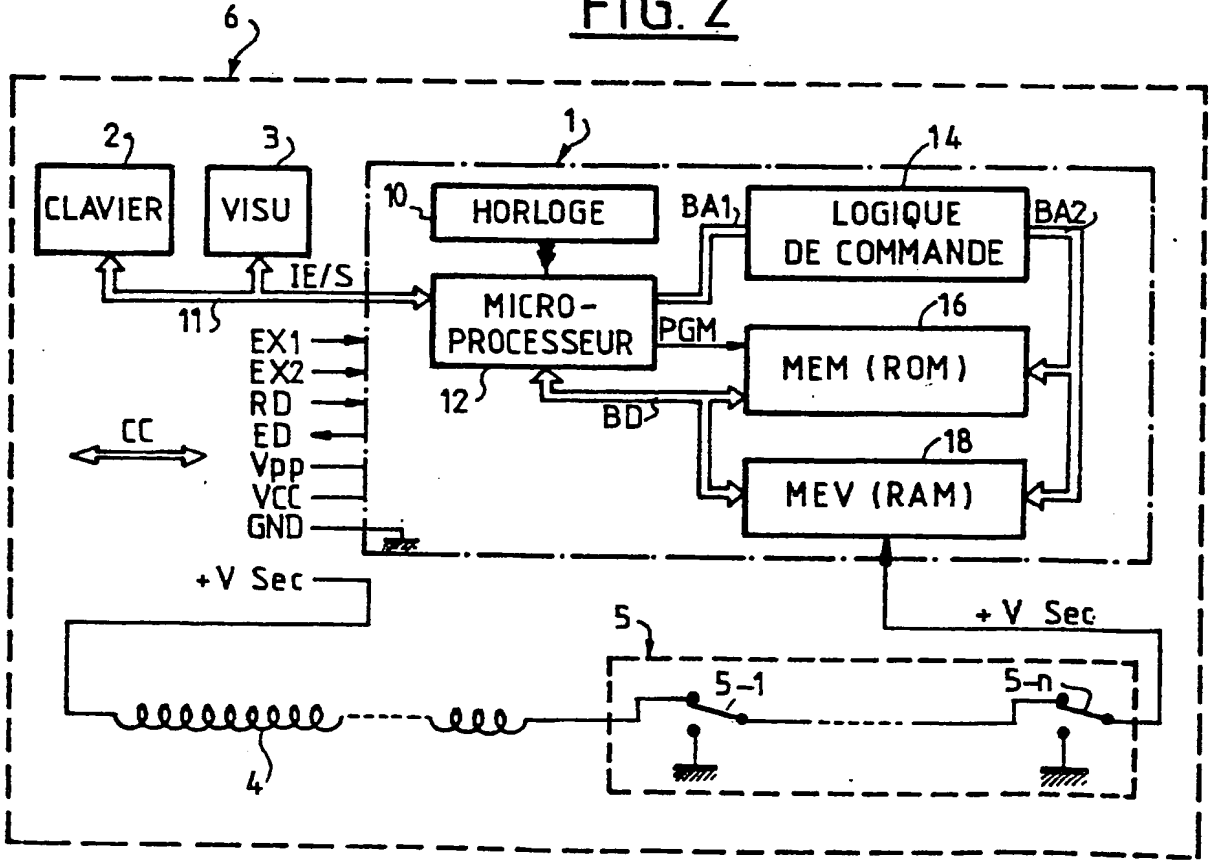


FIG.3A

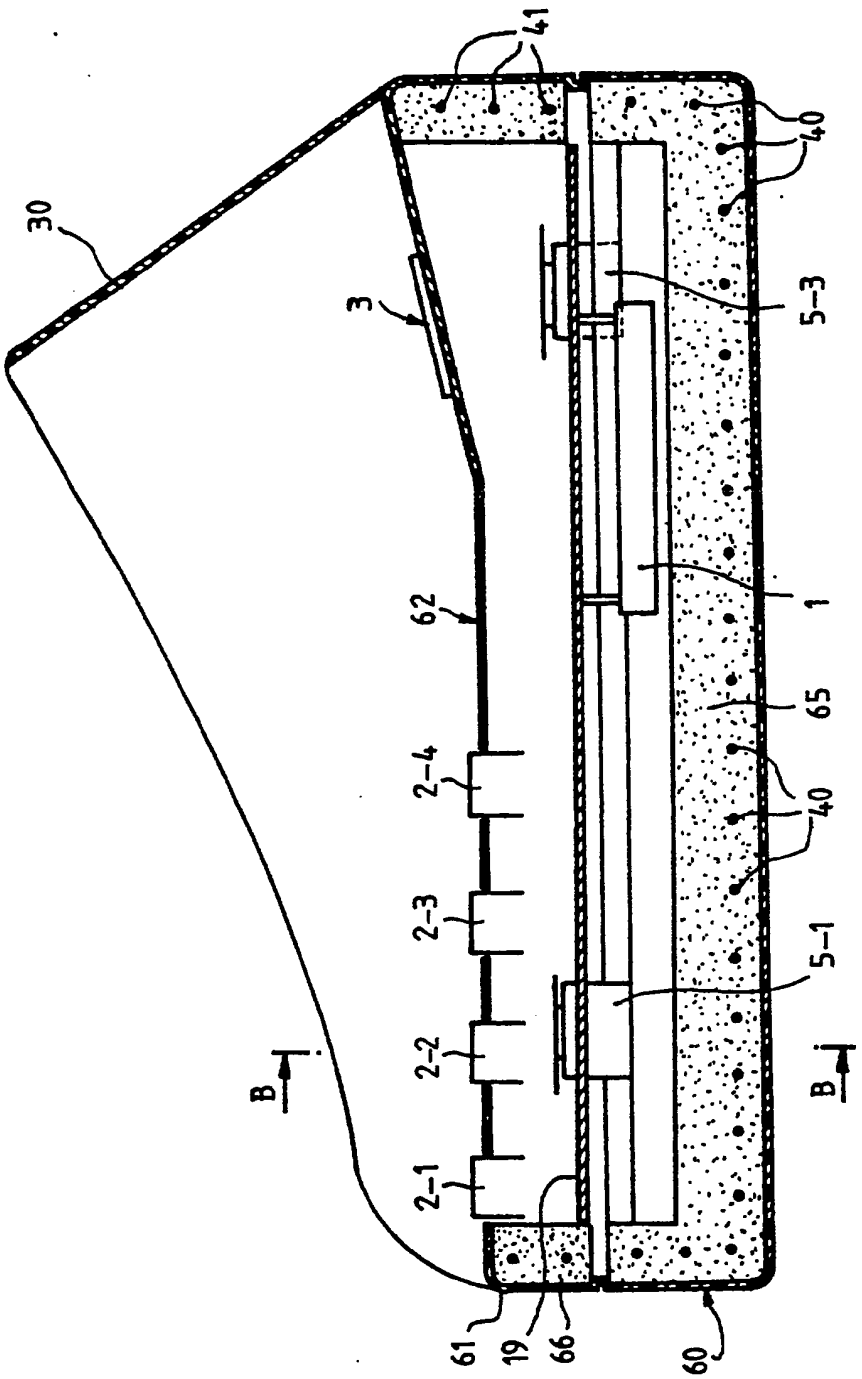


FIG. 3B